Minutes from Meeting on September 10, 2008

Meeting called to order: 1:30 PM at the Judicial Building

Persons in attendance:

Steve Mosena DHS
Alison Radl DAS-ISO
Calvin Moore DAS-ISO
Greg Fay DAS-ISO
Don Harvey IVH
Shane Ludwig IUB
Scott Miller LSA
Linda Torgeson DOT
Kevin Kammermeier DPS
Mark Wise IDR
Ruth Coleman IDR
Michael Chesmore DAS-ISO
Deb Castillo IVRS
Deb Covington DOT
Brent McManus ILOT
Carl Martin IWD
Bernie Zylstra IVRS

Agenda

Executive IT Security Briefing

Update on Enterprise solution for email encryption

Security Event and Information Management Project – FY09 Pooled Tech Project

Enterprise Wireless LAN Standard – Discussion of proposed changes

Enterprise Compliance Standard – Discussion of proposed standard

Open Discussion

Meeting Points

Executive IT Briefing (Video): Mike Coon has made quite a bit of progress on the video. There is some work remaining but Mike hopes to be done by the end of the month. If the video is complete it will be shown at the October meeting.

Email encryption: No update available.

Security Event and Information Management Project (SEIM):

Pooled tech funds (approximately $179,000) were made available for a SEIM project to identify software for log monitoring, analysis and alerting. The funds will be used to identify agency needs, select a product, and make an initial software purchase. The ISO will be asking for agency input on the project.

DOT is looking at purchasing SEIM software by the end of the year. One of the products that they are looking at is QRadar. The ISU Information Assurance Center will assist DOT with the selection of their software.

Enterprise Wireless LAN Standard

Will home wireless be addressed in this standard? No that should be part of a separate standard/policy.

Is SSID broadcasting still part of the standard? No, that section was removed.

#7 Range. Suggest adding the words "where practical".

What is the intent of the standard? Does it cover network to network wireless or client to network wireless? It covers client to network wireless.

What about wireless between buildings? This is a wireless LAN standard not WAN standard. A wireless WAN standard could be developed later if needed.

What is the process for reviewing/approving Enterprise Security Standards?

- The initial draft of the standard is shared with the CIO Council Security Subcommittee and the standard is revised based on the group's input.
- The revised draft is then shared with all agency CIOs and revised based on their input.
- The revised standard then goes to the TGB Standards workgroup for review and is updated based on their input.
- TGB reviews and votes on the final draft of the standard.

Enterprise Compliance Standard

The TGB has expressed a desire for more enforcement of the Enterprise Security Standards. This standard was drafted as a result.

Suggestion: Add a third check box on the Compliance Certification form for agencies with variances. For example, "Compliant with a variance." Note: The TGB wants to limit issuance of variances to those situations where it is clearly warranted.

What if agencies do not have the funding to comply with the standards? If funding is the sole reason for non-compliance that issue would go to the TGB.

Agencies will need a tool (i.e. checklist) to help them identify if they are compliant.

Will agencies need to do a risk assessment if they complete the Compliance Certification? The risk assessment and compliance certification address two different issues. The risk assessment helps the agency identify security risks faced by the agency. The Compliance Certification assigns responsibility for compliance with security standards. The Certification will bring security to the attention of agency heads.

How often will the Compliance Certification be completed? Annually

Who signs the Compliance Certification? The agency director/head.

Open Discussion

Mobile Device Standard: There was a discussion about implementation of the Mobile Device Standard which went into effect July 31, 2008.

Concern was expressed with the current inactivity timeout setting for some non-BlackBerry devices and possible disruption of service due to patching.

Agencies can meet with the ITE messaging team to discuss the settings for devices used by their employees.

Is there duplication in the standard? Specifically sections:

7. Short Message Service (SMS): Confidential information shall not be sent by SMS.

8. Peer to Peer Messaging (PIN to PIN): Confidential information shall not be sent by peer-to-peer messaging.

14. Bluetooth: The following settings are required for devices using Bluetooth:

a. Disable Discovery Mode,

b. Pairing,

i. Attempts to pair devices require prior management approval,

ii. If prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators,

iii. The Bluetooth functionality should be turned off unless a hands-free environment is required,

iv. Data sent between paired devices must be encrypted.

Items 7, 8 and 14 cover different things.

Item 7 (SMS) covers text messaging. BlackBerry devices do not encrypt text messages.

Item 8 (PIN to PIN) covers messages sent directly from one BlackBerry device to another when the PIN of that device is known. PIN to PIN messages bypass the BlackBerry Enterprise Server. PIN messages are encrypted however all BlackBerry devices share the same key. PIN message encryption does not prevent a BlackBerry device other than the intended recipient from decrypting the PIN message.

Item 14 (Bluetooth) - Bluetooth wireless technology enables Bluetooth enabled BlackBerry devices to establish a wireless connection with devices that are within a 10-meter range. Bluetooth enabled BlackBerry devices can connect to other Bluetooth enabled devices such as a hands-free car kit or wireless headset.

DAS-ISO is planning training opportunities for October (Cyber Security Awareness Month).

October 9 Technical Training at the Hoover Building
October 28 Security Awareness Training at the Wallace Building

An email will be sent out to agencies with details about the training.

A session targeted at managers was requested.

Some agencies have locations across the state. Providing training to those users is difficult. Can the ISO tape their training?

Shane Ludwig shared his confidentiality statement with the group.

The group had a discussion about working from home. Should agencies allow staff to use personal equipment when working from home? A future topic for discussion by the group: how can state workers work from home securely?

Meeting Adjourned: 3:00 P.M.

Next Meeting: October 8, 2008 1:30 P.M. – 3:00 P.M. Judicial Building